

Seminar

Overview of Functional Encryption and its Applications

Functional Encryption (FE) is an abstract term for public-key cryptosystems that differ from conventional encryption schemes: By using a secret key, the decryption procedure returns a function of the plaintext instead the plaintext itself. In addition to that, FE schemes rely on a trusted authority that generates secret keys for different users and different functions.

The goal of this work is to present the different types of Functional Encryption and its to give an overview of its applications.

References:

- Boneh D., Sahai A., Waters B. (2011) Functional Encryption: Definitions and Challenges. In: Ishai Y. (eds) Theory of Cryptography. TCC 2011. Lecture Notes in Computer Science, vol 6597. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19571-6_16

Contact

[Request Topic](#)

Advisors

Patrick Karl